O IMPACTO DOS CRIMES VIRTUAIS NA ATUALIDADE

Emily Duarte Anjos[1]
Lorena Silveira Rezend Armond[2]

RESUMO

O presente trabalho, tem como objetivo enfatizar acerca dos crimes cometidos na Internet, a fim de entender sobre os perigos dos cibercrimes na sociedade atual que possui livre acesso às redes tecnológicas. O desenvolvimento das tecnologias de informação e também a generalização no uso das mesmas refletem na delinquência e na criminalidade, agora também no universo da web. Nunca se comentou tanto sobre crimes cibernéticos como nos últimos anos, e isso se deve, obviamente, ao uso cada vez mais massivo da Internet, celulares, computadores, entre outros, que ocasionaram no aumento de ferramentas utilizadas para a prática de crimes. Os crimes virtuais vêm se tornando um assunto comum devido à grande facilidade em que essa prática ilícita vem sendo cometida, sendo esses tipos ilícitos caracterizados por falsidade ideológica, invasões em sistemas privados (Bancos), roubos de dados pessoais e muitas outras condutas que o Código Penal vem incluindo como prática desse crime. As leis estão se desenvolvendo e se adaptando às situações que este crime tem criado, buscando uma maior proteção à sociedade que hoje depende desses meios de informação e comunicação para quase tudo. Esta pesquisa aborda a necessidade de aplicação de meios de prevenção e proteção diante da prática do cibercrime.

Palavras-chave: Internet. Crimes virtuais. Cibercrimes. Leis.

1 INTRODUÇÃO

Frente ao grande avanço da tecnologia atualmente, a Internet foi uma das ferramentas que mais proporcionou novos recursos e funcionalidades. Por mais que tenha contribuído trazendo benefícios para a evolução da tecnologia, também abriu portas para que pessoas mal-intencionadas usem esses recursos para enganar pessoas, roubar informações e dinheiro.

Sabe-se que os crimes de Internet evoluíram no mesmo ritmo que as demais tecnologias, existindo uma gama imensa de novos tipos de ataques. Assim como no mundo real, no mundo virtual também vem sendo reproduzidas as práticas de crimes e novas condutas lesivas, multiplicando os casos envolvendo crimes cometidos através da Internet.

Os especialistas que desenvolvem meios de combater esses ataques sempre estão um passo atrás dos criminosos, pois estes desenvolvem novas tecnologias diariamente, onde o objetivo é o mesmo, fraude o usuário. Atualmente, esses conceitos estão sendo revistos pois foi percebido que é necessário prever e combater fraudes antes mesmo que elas possam trazer prejuízos para a sociedade em geral.

---

[1] Bacharela em Direito pela Faculdade de Ipatinga.

[2] Graduada em Ciência Econômicas pela PUC/MG - Graduada em Direito pela FADIPA – Pós-graduada em Metodologia do Ensino pela UNIVALE/MG.

Contudo, este trabalho acadêmico busca explorar bibliograficamente registro acerca de métodos de proteção de dados e informações que podem evitar diversos tipos de ataques que os usuários não têm conhecimento, mesmo ainda não sendo o bastante. O uso de novas práticas mais críticas ao utilizar a Internet pode ajudar a combater esses tipos de crimes, tendo em vista que muitas das questões relacionadas a essa prática podem ser tratadas pelos próprios usuários, já que não existe outra forma de fazer isso sem que seja procurando conhecer o assunto, por meio de programas de incentivo do governo ou até mesmo por pesquisas realizadas na própria Internet para entender melhor acerca dos riscos e formas de evitá-los.

No decorrer deste artigo será explicado todo o início, desde a criação da Internet, até a inclusão das práticas criminosas dentro do mundo virtual, abordando os programas utilizados pelos criminosos que praticam essa conduta ilícita, incluindo a história de um dos grandes criminosos que marcou todo o mundo.

No terceiro capítulo será conceituado o que é o crime virtual, o que pode ser entendido como um crime cibernético, serão analisadas as classificações desses tipos de crime e os sujeitos ativos e passivos dentro da conduta ilícita, e também será explicado sobre as medidas de reconhecimento e precauções contra tais práticas.

Já no quarto capítulo, será abordada a previsão legal perante a prática dos crimes virtuais e a legislação existente, que, será analisado que pode não ser o suficiente para diante do grande avanço da Internet e com isso, o aumento das práticas delituosas que vem avançando sem que tenha uma legislação se concretizando na mesma proporção para uma melhor abordagem do tema.

Neste trabalho foi utilizado o método dialético para descrever e entender os crimes virtuais, analisando e conceituando as inúmeras práticas realizadas no meio virtual e o método dedutivo, que fornece uma visão crítica do entendimento da prática dos crimes virtuais.

Portanto, ao final do trabalho será possível esclarecer: as medidas legislativas atuais são suficientes para a proteção contra as práticas de crimes virtuais?

2 O INÍCIO DA INTERNET E A INTRODUÇÃO DOS CRIMES VIRTUAIS

Antigamente os meios de comunicação que existiam eram utilizados para fins científicos e governamentais. O uso de telefones e redes de computadores eram restritos aos cientistas e funcionários do Governo com o intuito de armazenar informações, porém, com o início da Guerra Fria os Estados Unidos procurava um meio de proteção às suas informações e uma estratégia de comunicação para que fosse possível transferir dados por longas distâncias durante esse período, sem que fosse interferido pelos ataques soviéticos, o qual surgiram as inovações que levaram à criação da Internet.

A origem da Internet se deu em meados do ano de 1960, com o objetivo de proteção à comunicação do Estados Unidos durante as guerras, onde então foi fundada a “Apanet” (Agência de Pesquisa Avançada de Rede) como forma de privatizar e manter sigilosas as comunicações realizadas no país. Mas com o tempo e aprimoramento dela foi desenvolvido o protocolo TCP/IP onde a Internet passou a fazer parte de todos os âmbitos da sociedade, permitindo o acesso à comunicação instantânea a distância entre os usuários.

Por volta do ano 1985, os Estados Unidos criou o Sistema “NSFnet”, que junto com a “Apanet” tornou a Internet o principal meio de comunicação para redes individuais, educacionais e comerciais com alcance global. Com essa chegada da transformação digital houve o desenvolvimento e surgimento da educação virtual, do comércio eletrônico e do marketing digital. Já em meados da década de 90 a Internet se transformou em uma ferramenta indispensável, evoluindo cada vez mais.

A Internet é a maior inovação tecnológica dos últimos tempos. O seu crescimento nos proporcionou um amplo acesso às informações do mundo todo e de todos os

assuntos, gerando novas formas de comunicação e fácil obtenção acerca de qualquer assunto. Da mesma forma que sua expansão vem contribuindo de forma positiva, colaborando com o grande avanço da população em um todo, o fácil acesso informações pela Internet também facilitou a ação de criminosos que a utilizam para atividades ilícitas, aumentando o número de cibercrimes, já que, pela grande evolução tecnológica os criminosos obtém meios de dificultarem suas buscas e rastreamento até eles, tendo em vista que hoje em dia é capaz de realizar um crime virtual através do outro lado do mundo.

A partir do momento em que a internet implantou a tecnologia como forma de permitir a interação entre dispositivos, os crimes virtuais ganharam mais potencial. Segundo Marcelo Lau, coordenador do MBA em Cibersegurança do Centro Universitário FIAP: “O invasor tradicional é como um batedor de carteira digital”.

O espaço virtual vem aumentando os meios de aproximar as pessoas, permitindo que todos conectados a rede de Internet possam ter contato imediato com outra pessoa em qualquer lugar do mundo, beneficiando principalmente o crescimento econômico, já que todos os dias se convive com o comércio virtual, utilizando de operações bancárias, consultas à notícias e pesquisas através dela.

A utilização da rede mudou todas as atividades que realizadas, da mesma forma que trouxe benefícios ao mundo, a proporção de práticas ilícitas dentro dela causam danos á seus usuários, isso se dá pela facilidade de comunicação entres eles, o que tornou os crimes praticados dentro da Internet muito mais danosos do que no início dela, já que na atualidade é difícil controlar e identificar a origem da prática criminosa, tornando-se um desafio monitorar e se precaver durante a utilização da rede em computadores e eletrônicos.

2.1 Programas Criminosos

Para realizar as práticas criminosas são utilizados o computador e a Internet, principalmente o programa de computador chamado Software. Os Softwares mais conhecidos são os vírus, os cookies, o cavalo de Tróia, o sniffer, os spammings, os spywares e os hoaxes.

Os vírus são os meios mais conhecidos, tanto que há diversos programas “antivírus” utilizados atualmente. O invasor consegue atingir programas e configurações de computadores, tendo acesso a todas as informações contidas neles, através de links, vídeos, e-mails, dispositivos USB e programas infectados.

Os cookies, também muito comuns, são pacotes de dados enviados de sites para o navegador do usuário, tendo acesso às informações e atividades dele, inclusive senhas e dados de cartões cadastrados por esse usuário.

O cavalo de Tróia e o sniffer são programas espiões, que invadem softwares dos computadores com a finalidade de coletar informações, arquivos e senhas contidos no computador invadido. No cavalo de Tróia, quando instalado, por meio de arquivo criminoso, é invadido pelo criminoso que controla o computador, podendo copiar e excluir todos os arquivos existentes.

Os spammings são programas que enviam mensagens eletrônicas com finalidade de invadir a sua privacidade e sobrecarregar a caixa eletrônica, sem precisar da solicitação dos usuários, possibilitando a introdução de cookies, que, como foi dito anteriormente, podem ter acesso às informações do usuário.

Os spywares conseguem retirar todas as informações do computador do usuário, transmitindo para outro usuário de outra rede, sendo introduzido através de website acessado que possua o programa espião.

Já os hoaxes, são meios utilizados para enviar emails com conteúdos sentimentais, dramáticos ou religiosos, se passando por empresas ou órgãos governamentais, com finalidade de causar comoção social e espalhar “fake news” acompanhada de vírus.

2.2 Caso: Hacker Kevin Mitinick

Um dos marcos históricos dos crimes cibernéticos mais famosos foi o caso do hacker Kevin Mintick, um dos hackers mais famosos do mundo, que, após ser procurado pelo FBI pelas suas práticas criminosas, acabou se tornando um “hacker do bem”, trabalhando para o governo americano na área de segurança de informação e se tornando consultor de cibersegurança, utilizando de suas habilidades para prestar serviços a empresas e instituições governamentais, sendo ainda fundador da empresa KnowBe4, conhecida por ser provedora do maior treinamento de conscientização de segurança do mundo.

Na época que Kevin começou a praticar os crimes utilizando as redes, foi iniciada uma caça do governo norte americano para conseguir achá-lo, sendo que, após muitos anos de procura ele foi encontrado e punido pelas invasões e crimes cometidos e posteriormente se tornou um exemplo e tomou posse de cargo importante para a segurança do governo americano. Entre os crimes por ele praticado pode-se citar roubos de informações de cartões de créditos, roubos de dados e de informações confidenciais de operadores de telefonias.

As práticas de Kevin começaram bem cedo, ainda jovem ele conseguiu burlar o sistema de ônibus da cidade em que morava, Los Angeles, para utilizar o transporte sem precisar pagar, apenas utilizando um furador de cartões e passagens de baldeação que ele encontrou em um lixo.

Uma das primeiras atividades cometidas por Kevin que tomou grande proporção, foi na década de oitenta, quando aos 16 anos ele começou a se interessar por computadores, e, como tudo ainda era muito novo, não era de se imaginar que as práticas delituosas começariam a ser praticadas nesse meio virtual.

Com apenas essa idade, o jovem Kevin conseguiu invadir os sistemas de computadores e copiar códigos de uma empresa conhecida por ser uma das pioneiras do mercado de informática dos Estados Unidos, a empresa DEC - Digital Equipment Corporation. A partir de então, ficou conhecido por seus ataques direcionados a empresas que utilizavam técnicas de engenharia para obtenção de informações confidenciais.

Ao ser condenado pelo episódio da DEC, no final de sua pena ele realizou uma invasão na empresa Pacific Bells, uma das maiores empresas operadoras de telefonia dos Estados Unidos, se tornando a partir daí um dos maiores procurados pelo FBI.

Em 1995, o FBI conseguiu capturá-lo e então ele declarou a sua culpa em várias práticas cibernéticas criminosas. As atividades praticadas por Kevin se tornaram muito famosas, incentivando a criação de legislações que abordam os crimes digitais, já que na época os crimes relacionados às redes não possuíam tipificações, servindo de alerta também sobre os riscos que essas novas tecnologias trariam à sociedade.

Após ser condenado por suas práticas em meados do ano 2000, ele também foi proibido de utilizar qualquer tipo de tecnologia no período em que esteve em liberdade supervisionada, o que incentivou o hacker a “mudar de lado” e utilizar seus conhecimentos para práticas de segurança, ficando então conhecido por se tornar um grande escritor de livros e criador de conteúdos acerca de práticas para melhoria de segurança no mundo cibernético.

3 CRIMES VIRTUAIS

O cibercrime, também conhecido como crimes virtuais ou crimes cibernéticos, nada mais é que atos criminosos realizados por meio da Internet e redes conectadas a computadores e dispositivos eletrônicos nos ambientes virtuais por meio da tecnologia da informação. A INTERPOL (2015) conceitua o cibercrime como atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na Internet.

O termo “cibercrime” foi originado no fim da década de 1990 após uma reunião do grupo G8, conhecido por ser o conjunto dos oito países mais desenvolvidos e

influentes do mundo (Rússia, Estados Unidos, Canadá, Itália, França, Alemanha, Japão e Reino Unido), que, realizaram uma reunião em Lyon, na França, para discutirem acerca dos crimes na Internet que na época, mesmo sem muita evolução da mesma, já aconteciam, com o intuito de introduzir formas de prevenção e combate às práticas ilícitas.

A Internet, por ser no mundo atual a maior fonte e veículo de informações, também se tornou uma ferramenta perigosa, tendo em vista a facilidade de propagação de informações e notícias que podem ser falsas. Ela proporciona infinitos benefícios por ela ofertados, mas também inúmeros serviços e plataformas que podem ser prejudiciais e mal intencionados, os quais colaboram com o crescimento dos crimes virtuais na atualidade.

Esse tipo de crime pode ser praticado por uma pessoa ou por um grupo, por meio de fraudes e golpes através da obtenção de dados pessoais ou bancários da vítima, muitas vezes com o intuito de coletar ou até mesmo destruir informações confidenciais a fim de obter compensação financeira em troca.

A grande diferença dos crimes virtuais para os crimes comuns é a não utilização de barreiras físicas ou geográficas, podendo ser eles cometidos com menos esforço e mais velocidade e facilidade, dependendo do tipo de crime praticado.

3.1 Classificação dos crimes virtuais

Os crimes virtuais podem ser classificados pelo sujeito ativo e sujeito passivo e como crimes próprios ou crimes impróprios.

Para a classificação de sujeito ativo são utilizadas as denominações “hacker” e “cracker”. O “hacker” são as pessoas que utilizam de seus conhecimentos para ganhar acesso a sistemas privados, normalmente são pessoais com grandes conhecimentos informáticos que podem ser utilizados de forma positiva ou negativa, não necessariamente apenas para as práticas ilícitas.

Já os “crackers” são aqueles que, diferente dos “hackers”, utilizam de seus conhecimentos para atividades criminosas com o objetivo de obter vantagens ilícitas, utilizando de ações ilegais que causem transtornos para outras pessoas.

Além deles, pode-se citar os pherakers que são utilizam de linhas telefônicas e aparelhos celulares clonados para realizar ligações clandestinas e realizar ataques como golpes e a sistemas externos, enviando sms para confirmação e conseguir acessar o aparelho celular da vítima.

Quanto aos sujeitos passivos, evidentemente será alguém que está sendo lesado e sofrendo com a ação praticada. Nos casos dos crimes virtuais, poderá ser uma pessoa física ou jurídica ou uma entidade pública ou privada titular do bem jurídico tutelado. As pessoas físicas que são vítimas dos crimes virtuais ainda não possuem tantos mecanismos de proteção jurídica, devido ainda a falta de punibilidade aos infratores e falta de mecanismo para as denúncias. Já as empresas que são vítimas, optam por evitarem a divulgação dos ataques para não demonstrarem possíveis fragilidades quanto à sua segurança.

Ao se classificar um crime virtual próprio, analisa-se primeiramente os sujeitos e a ação realizada. Normalmente, neste caso o sujeito ativo utiliza de seus conhecimentos para invadir o sistema de computador da vítima para a prática do crime, violando o bem jurídico protegido pela norma penal.

Os crimes virtuais classificados como impróprios são aqueles realizados por meio de computador para a prática de condutas ilícitas para produzir resultado que prejudique o mundo físico, podendo haver ameaça ou lesão a outros bens sem ser apenas os virtuais.

3.2 Condutas e prevenções

Quando houver a suspeita de que a vítima caiu em uma fraude de crime cibernético a primeira providência a ser adotada é a coleta de comprovações do possível golpe, quanto mais informações tiver mais fácil será a adoção de medidas. Prints, arquivos, conversas, e-mails ou qualquer outra comprovação será necessária. Em alguns casos, o registro desses documentos ajudam a comprovar a sua veracidade. E, para adoção de medidas judiciais, a realização de boletim de ocorrência na delegacia de polícia para registro do crime dará início às investigações.

Observa-se que, por ser uma prática de crime “recente”, não são todos os Estados que possuem Delegacias especializadas para este tipo de crime, mas, as polícias do mundo todo vêm se preparando cada vez mais, com ferramentas de última geração para o combate e inibição dessa prática criminosa

A melhor forma de se proteger é desconfiando sempre. Pode-se considerar que existem várias maneiras de aplicar a segurança no mundo digital, focando em sempre atentar-se aos golpes a fim de evitar ser vítima desses crimes virtuais, podendo elas serem realizadas pelos próprios usuários de forma prática e fácil.

Algumas das medidas que podem ser tomadas como precaução da exposição de dados pessoais se dão pela atenção a legitimidade e segurança dos sites, conferindo sempre o URL, a criação de senhas fortes que se alternam entre letras, números e símbolos e que não possuam informações ou dados pessoais como datas, a utilização da autenticação de dois fatores nos aplicativos, a atenção ao abrir links, arquivos ou e mails desconhecidos, o não fornecimento de dados pessoais por telefone ou meios de comunicações que não sejam confiáveis, a atenção aos extratos bancários, além dessas medidas ainda existem muitos outros meios de atenção e cuidado que podem ser tomados como prevenção da prática de crimes praticados na Internet.

3.3 Tipos de crimes virtuais

Conforme o mundo virtual vem se desenvolvendo e crescendo, o número de práticas criminosas que podem ser realizadas através da mesma também vem criando grandes avanços. Há os crimes virtuais mais conhecidos, como o bullying, a pedofilia, o roubo de dados, o estelionato, as ameaças, porém, além dessas práticas mais “comuns”, na atualidade vem sido necessária uma maior preocupação com as práticas realizadas pelos hackers, através das redes e sistemas, as quais vêm causando diversos prejuízos já que o acesso aos dados de usuários e empresas tem ficado cada vez mais comprometidos com o aumento dessas práticas criminosas.

Pode-se citar algumas práticas que precisam de maiores estudos e medidas de prevenção, como:

● **Phishing**: pode-se dizer que é uma das formas mais utilizadas para a prática de crime virtual no Brasil. O nome é uma referência a “pesca”, ou melhor interpretando, “isca digital”. A prática é realizada através de acesso a anúncios de dinheiros e oportunidades fáceis, como spam, e-mail e mensagens que, ao serem acessadas, permite o compartilhamento dos dados contidos na rede da vítima ao criminoso.

Dentro do Phising também há a prática Spearphising. A diferença dessa prática é que, em vez de se passar por uma empresa, como explicado acima, o criminoso se passa por alguém próximo da vítima, facilitando que ela confie em acessar o arquivo que o fará ter acesso a seus dados.

● **DDoS** (ataque de negação de serviço): essa prática é realizada pelos cibercriminosos, geralmente com o intuito de causa danos contra empresas, através de técnicas avançadas que permitem o interrompimento de sistemas de uma rede, sobrecarregando os servidores, podendo deixá-los até mesmo fora do ar, sendo que, assim que ocorre esse interrompimento, os criminosos conseguem solicitar pagamentos, destruir e até mesmo vazar dados do sistema invadido.

Em 2011 aconteceu o Caso Sony, um grande exemplo da prática do DdoS, onde criminosos conseguiram vazar dados de aproximadamente 77 milhões de usuários da PlayStation, causando grandes prejuízos financeiros à empresa pelos dias em que a mesma ficou fora do ar, tendo que fornecer benefícios a todos os usuários prejudicados.

● **Ransomware**: é uma prática que pode ser considerada um vírus, onde é realizado através de envio de mensagens simulando conteúdos reais por hackers para usuários de algum sistema, normalmente o foco é sistemas de empresas, fazendo com que o usuário acesse o arquivo infectado. Ao ser acessado, o ransomware consegue realizar uma varredura na rede da empresa até que consiga ter acesso aos sistemas internos e privados dela, resultando no bloqueio de dados da empresa. Após, os criminosos exigem pagamentos para que liberem o acesso à empresa que foi atingida pela prática criminosa. Vale ressaltar que, caso a empresa tente retomar o acesso por conta própria, eles correm o risco de terem seus dados apagados pelos criminosos.

Em 2013 houve o Caso Microsoft, onde computadores que utilizavam os sistemas operacionais Windowns foram infectados pelo ransomware, que conseguiu obter acesso a chaves criptografadas da empresa, acumulando um prejuízo de cerca de 3 milhões de dólares.

● **Malware**: essa prática é realizada através de hackers que infectam o computador ou a rede, com o objetivo de roubar dados e até mesmo realizar outros tipos de ataques, esse acesso ao sistema se dá através de arquivos e links infectados, no qual, assim que abertos, dão acesso aos criminosos para o dispositivo da vítima.

Além das modalidades de crimes virtuais classificadas acima, pode-se mencionar também os crimes praticados na “vida real” que estão previstos na legislação brasileira mas que ocasionalmente também são classificações para as práticas criminosas cometidas no ambiente virtual, como os crimes de inserção de dados falsos em sistemas de informações (art. 313-A, CP), contra a liberdade individual (art. 153, § 1º-A, CP), ameaça (art. 147, CP), injúria (art. 140, CP), calúnia (art. 138, CP), difamação (art. 139, CP), racismo (art. 20, da Lei 7.716/89), apologia ao crime (art. 287, CP), incitação ao crime (art. 286, CP), lavagem de dinheiro (Lei 9.613/98) e quadrilha ou bando (art. 288, CP).

4 APLICAÇÃO DAS LEIS NOS CIBERCRIMES

Devido ao grande avanço da Internet houve consequentemente o avanço dos crimes virtuais, e infelizmente as condutas de aplicações das Leis diante desses crimes não vem avançado da mesma forma. Contudo, o Direito vem se adaptado a essa nova realidade, a realidade do mundo virtual, procurando avançar em todos os seus ramos para se adaptarem e conseguirem aplicar as leis dentro das práticas virtuais.

Pode-se dizer que o Brasil se encontra de certa forma atrasado, tendo em vista que é imprescindível o desenvolvimento de leis mais severas e específicas para combater os crimes virtuais, e, o ordenamento jurídico brasileiro é falho nisso e utiliza leis secundárias para punição desses tipos de casos. Mesmo ainda não possuindo condutas e tipificações adequadas para aplicações de leis aos cibercrimes, o país começou a se adequar ao mundo virtual a partir do aumento das inovações tecnológicas entre a população, procurando promulgar regras e leis relativas à competência do Estado em razão dos crimes virtuais.

Mesmo com a criação de Leis como a 12.737/2012, promulgada após o caso Carolina Dieckman que teve suas informações e arquivos roubados e expostos, a sanção do Marco Civil da Internet, e algumas outras leis que possam ser aplicadas de formas menos específicas, o país ainda continua sem uma adequada tipificação para monitorar esse aumento de casos de crimes, não sendo suficientes as leis já existentes.

Os crimes que estão previstos na legislação brasileira ainda não são suficientes para classificar e regulamentar todos os crimes que vêm sido cometidos no meio virtual, por meio das redes, necessitando de definição de leis especiais para poder dar uma garantia da ordem legal e social para a sociedade.

4.1 Lei 12.695/2014 (Marco Civil da Internet)

A Lei 12.965/2014, conhecida como “Marco Civil da Internet”, foi sancionada com o objetivo de definir diretrizes para o uso da Internet no país, promovendo a liberdade de expressão, privacidade dos usuários, a neutralidade de rede e a responsabilidade dos provedores de Internet e serviços online. É uma legislação brasileira que estabelece princípios, direitos e deveres para o uso da Internet no Brasil. O primeiro artigo da Lei diz: “Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.”

A criação da Lei teve um papel significativo na regulamentação da Internet no Brasil, buscando equilibrar a promoção da inovação e liberdade online com a proteção dos direitos dos usuários e da sociedade em geral.

Alguns dos princípios abordados pela Lei são:

- **Neutralidade de Rede:** O princípio da neutralidade de rede assegura que os provedores de internet não podem discriminar, bloquear, monitorar ou interferir no tráfego de dados, garantindo que todos os conteúdos e serviços sejam tratados igualmente.
- **Privacidade e Proteção de Dados:** A lei estabelece a proteção da privacidade dos usuários e a necessidade de obtenção de consentimento explícito para coleta, armazenamento e compartilhamento de dados pessoais.
- **Liberdade de Expressão:** O Marco Civil garante a liberdade de expressão dos usuários, mas também estabelece limites para conteúdos que violem direitos humanos e outros valores fundamentais.
- **Responsabilidade dos Provedores de Serviços:** A legislação determina que os provedores de internet e serviços online não são responsáveis pelo conteúdo gerado pelos usuários, a menos que não cumpram ordens judiciais específicas para a remoção de conteúdo ilegal.
- **Armazenamento de Dados:** A lei estabelece que os provedores de conexão e aplicativos devem guardar registros de acesso dos usuários por um período de tempo, a fim de fornecer informações para investigações criminais.
- **Proteção ao Consumidor:** O Marco Civil da Internet também traz disposições para a proteção dos direitos dos consumidores online, garantindo transparência nas relações de consumo na internet.

4.2 Lei 12.737/2012 (Lei Carolina Dieckman) e Lei 12.735/2012 (Lei Azeredo)

No ano de 2011 a atriz Carolina Dieckman teve seu computador invadido por um criminoso virtual, conhecido também como “hacker”, o qual teve acesso a fotos íntimas da atriz e tentou suborná-la para que o pagasse a quantia de R$ 10.000,00 (dez mil reais) para que suas fotos não fossem divulgadas. Diante da recusa do pagamento, a atriz teve suas fotos vazadas, o que criou um escândalo no país.

Um ano após o ocorrido, em 2012, foi sancionada a Lei 12.737 com o nome da atriz, que abraçou a causa já que na época do ocorrido não teve amparo legislativo específico para a devida penalização dos criminosos: “Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.”

A Lei prevê a segurança no ambiente virtual, conforme o art. 2º, acrescentou os artigos 154-A e 154-B ao Código Penal:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)

> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012).

A inclusão dos artigos ao Código Penal deu abertura à tipificação dos crimes virtuais, como a invasão de dispositivos informáticos com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do proprietário.

Quanto à Lei 12.735/2012, esta foi sancionada para determinar aos órgãos de polícia a criação de setores e equipes especializadas no combate aos delitos em redes de computadores e dispositivos de comunicação:

> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

4.3 Lei 13.709/2018 (Lei Geral de Proteção de Dados)

A Lei Geral de Proteção de Dados aborda acerca do tratamento de dados pessoais de pessoa natural ou pessoa jurídica de direito público ou privado, inclusive pelas plataformas digitais, objetivando a proteção dos direitos fundamentais de liberdade e de privacidade delas:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência.

A Lei, sancionada em 2018, fundamenta acerca da liberdade de expressão, assegurando ao cidadão o direito de proteção aos seus dados pessoais e íntimos, a respeito dos direitos humanos, visando o livre desenvolvimento de personalidade, dignidade exercício de cidadania de todos, o respeito à privacidade de todos os cidadãos, assegurando os direitos fundamentais de inviolabilidade íntima, da honra, da imagem e da vida privada, o desenvolvimento económico e tecnológico e a livre iniciativa e concorrência.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;

> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

5 CONCLUSÃO

Ao longo da jornada desse trabalho, foi possível aprofundar a análise acerca dos impactos que as redes sociais vêm causando na sociedade. Como se pode observar, a Internet vem crescendo de várias formas, principalmente por ter se tornado o mais importante meio de comunicação do mundo. Assim, na mesma forma em que a Internet vem nos proporcionando inúmeros benefícios, ela também vem possibilitando o aumento das práticas ilícitas que podem prejudicar seus usuários.

Buscou-se entender que os crimes virtuais são aqueles praticados com o uso específico da Internet e da tecnologia por práticas ilícitas que causam danos à alguém ou a algo .

Um assunto que foi muito abordado ao longo da pesquisa foi a questão de ser necessário tomar as medidas protetivas necessárias para evitar a facilidade da prática dos crimes virtuais, por isso, foi esclarecido ao longo do texto formas de proteção e prevenção. Ainda dentro das práticas dos crimes virtuais, analisou-se um caso muito famoso mundialmente acerca do assunto, que foi o caso de Kevin Metnick, homem que ficou conhecido pelos atos infracionais cometidos pela Internet antes dos anos 2000, e que foi devidamente punido e responsabilizado por seus atos, o que influenciou na adequação de medidas aplicáveis a estes tipos de crimes.

Viu-se ao decorrer da pesquisa que a grande maioria dos crimes cibernéticos são praticados através da utilização de softwares, como o vírus, cookies, cavalo de troia, spammings, spywares e os hoxaxes. São várias as classificações dos agentes criminosos desses cibercrimes, sendo os mais conhecidos pelas práticas os hackers e os crackers. Podendo as práticas abordadas no artigo ocorrerem de forma própria, através dos conhecimentos do criminoso para invadir a rede/computador da vítima para a prática do crime, ou de forma imprópria, no qual a conduta praticada pelo computador prejudica o mundo físico e não apenas o virtual.

Atualmente não existem muitas condutas legislativas que possam ser aplicadas e tipificadas perante as condutas criminosas nos ambientes virtuais, o que acaba dificultando a punição aos criminosos, fazendo com que, pela falta de punibilidade, eles pratiquem cada vez mais os cibercrimes. Por mais que no Brasil tenham sido criadas leis que trouxeram grandes avanços aos direitos dos usuários da Internet, como a Lei do Marco Civil da Internet, as medidas a serem tomadas diante das práticas não são o suficiente para combater os crimes virtuais na mesma proporção em que eles vem crescendo.

Desse modo, por mais que já existam certas leis que possam ser aplicadas para punições nas práticas de crimes virtuais, essas medidas não são suficientes para classificar e regulamentar os crimes cometidos no meio virtual, portanto, conclui-se que ainda é necessário a criação e regulamentação de leis específicas para se conseguir combater os crimes virtuais e aumentar as medidas de proteção e segurança aos usuários, principalmente pelo fato da Internet ter se tornado essencial para todo o mundo.

REFERÊNCIAS

ALVES, Maria Hiomara dos Santos. A evolução dos crimes cibernéticos e o acompanhamento das leis específicas no Brasil. **Jus.com.br**, 18 mar. 2018. Disponível

em: https://jus.Com.Br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-o-acompanhamento-das-leis-especificas-no-brasil. Acesso em: 20 jul. 2023.

ANDRION, Roseli. História da segurança virtual: a origem do cibercrime. **CANAL TECH**, 29 nov. 2021. Disponível em: https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-cibercrime-203073/. Acesso em: 11 ago. 2023.

BRASIL. **Lei nº 12.695, de 25 de julho de 2012.** Dispõe sobre o apoio técnico ou financeiro da União no âmbito do Plano de Ações Articuladas; altera a Lei nº 11.947, de 16 de junho de 2009 [...]. Vigência. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12695.htm. Acesso em: 22 jul. 2023.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 22 jul. 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 jul. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) . Vigência. Brasília, DF: Presidência daRepública, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 22 jul. 2023.

BRASIL. Superior Tribunal de Justiça. **Justiça usa código penal para combater crime virtual**. 2008. Disponível em: https://stj.Jusbrasil.Com.Br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual. Acesso em: 18 jul. 2023.

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos:** noções básicas de investigação e ameaças na internet. Disponível em: http://www.conteudojuridico.com.br/artigo,crimes-ciberneticos-nocoes-basicas-de-investigacaoeameacas-na-internet,54548.html. Acesso em: 18 jul. 2023.

CIBERCRIME: o que é e como pode ameaçar as organizações. **NAVITA**, 2020. Disponível em: https://navita.com.br/blog/cibercrime-o-que-e-e-como-pode-ameacar-as-organizacoes/. Acesso em: 11 ago. 2023.

CIBERCRIME: o que você deve saber e como se prevenir. **MOBILIT**, 29 jul. 2021. Disponível em: https://www.mobilit.com.br/cibercrime-saiba-mais/. Acesso em: 11 ago. 2023.

DEMARTINI, Felipe. Quem foi Kevin Mitnick, o ex-hacker mais procurado do mundo. **CANAL TECH**, 20 jul. 2023. Disponível em: https://canaltech.com.br/seguranca/

quem-foi-kevin-mitnick-o-ex-hacker-mais-procurado-do-mundo-256728/. Acesso em. 18 ago. 2023.

D'URSO, Luiz Augusto Filizzola. **Cibercrime:** perigo na internet. 2017. Disponível em: https://politica.Estadao.Com.Br/blogs/fausto-macedo/cibercrime-perigo-na-internet/. Acesso em: 13 jul. 2023.

GARCÍA-PABLOS DE MOLINA, Antonio; GOMES, Luiz Flávio. **Criminologia:** introdução a seus fundamentos teóricos, introdução às bases criminológicas da Lei 9.099/95 - Lei dos juizados especiais criminais. 3. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2000.

KOVACS, Leandro. O que é um crime cibernético? 3 casos populares. **Tecnoblog**, 2021. Disponível em: https://tecnoblog.net/responde/o-que-e-um-crime-cibernetico-3-casos-populares. Acesso em: 18 ago. 2023.

LEI 'Carolina Dieckman', que pune invasão de PC's, entra em vigor. **G1, em São Paulo**, 02/04/2013. Disponível em: http://g1.Globo.Com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.Html. Acesso em: 13 jul. 2023.

LENZA, Pedro. **Direito constitucional esquematizado**. 16. ed. São Paulo: Saraiva, 2012.

MARCO Civil da Internet. **AURUM**, 1 jun. 2023. Disponível em: https://www.aurum.com.br/blog/marco-civil-da-internet/. Acesso em: 18 ago. 2023.

MASSON, Cleber. **Direito penal esquematizado, v.2:** parte especial. 9. ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método, 2016.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. **Revista Científica da FASETE**, v. 1, 2018.

NASCIMENTO, Anderson. O que é cibercrime. **CANAL TECH**, 11 jul. 2014. Disponível em: https://canaltech.Com.Br/seguranca/o-que-e-cibercrime/. Acesso em 15 de julho de 2023.

NASCIMENTO, Samir de Paula. Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais. **AMBITO JURIDICO,** 03 set. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/. Acesso em: 12 ago. 2023.

O QUE são crimes cibernéticos? Como se proteger dos crimes cibernéticos. KASPERSKY, 2023. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 12 ago. 2023.

SAMPAIO, Laire de Melo. Crimes virtuais: os limites da liberdade de expressão na Internet e a lei do esquecimento. **Conteúdo Jurídico**, 25 nov. 2021. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/57615/crimes-virtuais-os-limites-da-liberdade-de-expresso-na-internet-e-a-lei-do-esquecimento. Acesso em: 12 ago. 2023.

UGULINO, Márcio. Segurança na internet: saiba como evitar ser vítima de crimes virtuais durante a pandemia. **Instituto Federal da Paraíba. Campus João Pessoa**, 27 maio 2020. Diponível em: https://www.Ifpb.Edu.Br/joaopessoa/noticias/2020/05/seguranca-na-internet-saiba-como-evitar-ser-vitima-de-crimes-virtuais-durante-a-pandemia. Acesso em: 18 jul. 2023.

VIDAL, Rodrigo de Mello. **Crimes virtuais**. Rio de Janeiro: 2015. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/crimes_virtuais.pdf. Acesso em: 18 jul. 2023.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação. Rio de janeiro: Brasport, 2012.